

CLAIM LISTING

No claims have been amended, canceled, or added. A claim listing is provided as a courtesy.

1. (Previously Presented) A method of verifying a user in a health-related transaction, the method comprising:

receiving a request from a portable healthcare device to perform a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;

receiving biometric data from the portable healthcare device;

determining whether corresponding biometric data is stored;

if corresponding biometric data is stored,:

identifying a user associated with the corresponding biometric data; and

checking a credential service for professional license, professional license validity, and/or professional certification credential information associated with the identified user to determine whether the user is permitted to perform the requested health-related transaction; and

if the credential information is valid, sending to the portable healthcare device, enabling information for performing the health-related transaction.

2. (Original) The method of claim 1, wherein the request includes login information to initiate a session and the enabling information includes session information.

3. (Previously Presented) The method of claim 2, wherein checking credential information includes sending a request for a credential check to a credential service and receiving a credential check result from the credential service.

4. (Original) The method of claim 2, further including requiring the login information after a pre-designated time period of inactivity.

5. (Original) The method of claim 1, wherein the enabling information includes the credential information for forwarding to the remote information site.

6. (Previously Presented) The method of claim 5, wherein checking credential information includes comparing the credential information to previously determined credential information for a current session.

7. (Original) The method of claim 1, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data.

8. (Original) The method of claim 1, wherein if corresponding biometric data is not stored, further including denying the requested health-related transaction.

9. (Original) The method of claim 1, wherein the receiving biometric data occurs at pre-designated intervals of time.

10. (Previously Presented) A system for verifying a user in a health-related transaction, comprising:

- a) a biometric database to store biometric data;
- b) a biometric engine to determine whether corresponding biometric data is stored in the biometric database for a user of a portable healthcare device requesting a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;
- c) a credential request unit to determine validity of credential information associated with the user if corresponding biometric data is stored, the credential information including professional license, professional license validity, and/ professional certification; and

42P11777

Serial No. 09/967,211

- 3 -

Examiner: Greene, Daniel L.

Art Unit: 3621

d) an internal network port to receive the request for the health-related transaction from the portable healthcare device and to send enabling information for performing the health-related transaction to the portable healthcare device if the credential information is valid if the credential information indicates that the user is permitted to perform the health-related transaction.

11. (Original) The system of claim 10, wherein the request includes login information to initiate a session and the enabling information includes session information

12. (Original) The system of claim 11, further including an external network port to send a request for a credential check from the credential request unit to a credential service and receive a credential check result from the credential service.

13. (Original) The system of claim 10, further including a notification unit to send a requirement for the login information after a pre-designated time period of inactivity.

14. (Original) The system of claim 10, wherein the enabling information includes the credential information for forwarding to the remote information site

15. (Original) The system of claim 14, wherein the credential request unit is to compare the credential information to previously determined credential information for a current session.

16. (Original) The system of claim 10, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data.

17. (Previously Presented) A computer accessible medium having stored therein a plurality of sequences of executable instructions, which, when executed by a processor, cause the system to:

receive a request from a portable healthcare device to perform a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;

42P11777

Serial No. 09/967,211

- 4 -

Examiner: Greene, Daniel L.

Art Unit: 3621

receive biometric data from the portable healthcare device;

determine whether corresponding biometric data is stored;

if corresponding biometric data is stored,:

identifying a user associated with the corresponding biometric data; and

checking a credential service for professional license, professional license validity, and/or professional certification credential information associated with the identified user to determine whether the user is permitted to perform the requested health-related transaction; and

if the credential information is valid, send to the portable healthcare device, enabling information for performing the health-related transaction.

18. (Original) The computer accessible medium of claim 17, wherein the request includes login information to initiate a session and the enabling information includes session information...

19. (Original) The computer accessible medium of claim 18, wherein the determining of validity of credential information includes sending a request for a credential check to a credential service and receiving a credential check result from the credential service.

20. (Original) The computer accessible medium of claim 18, further including additional sequences of executable instructions, which, when executed by the processor further cause the system to require the login information after a pre-designated time period of inactivity.

21. (Original) The computer accessible medium of claim 17, wherein the enabling information includes the credential information for forwarding to the remote information site.

22. (Original) The computer accessible medium of claim 21, wherein the determining of validity of credential information includes comparing the credential information to previously determined credential information for a current session.

23. (Original) The computer accessible medium of claim 17, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data

24. (Original) The computer accessible medium of claim 17, further including additional sequences of executable instructions, which, when executed by the processor further cause the system to interrupt a processor to deny the requested health-related transaction if corresponding biometric data is not stored.

25. (Original) The computer readable medium of claim 17, wherein the receiving biometric data occurs at pre-designated intervals of time

Claims 26-29. (Canceled).